Artificial Intelligence & EU citizens/consumers

Hans Micklitz, Przemyslaw Palka
European University Institute
Giovanni Sartor
European University Institute, Cirsfid-University of Bologna

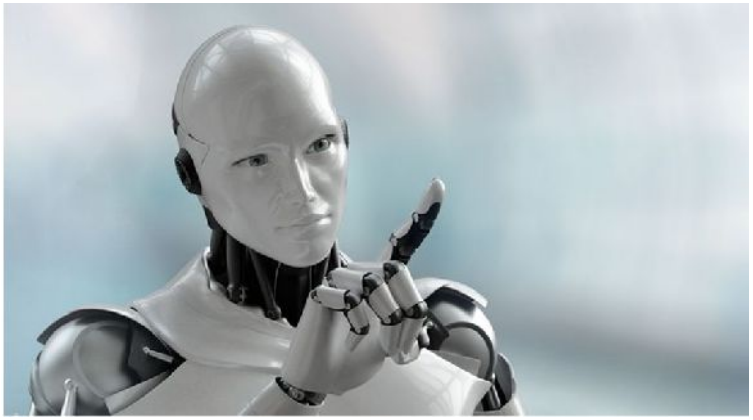
AI and the Internet: convergent evolutions

- Artificial intelligence reaches maturity
  - From human-made representations of knowledge and logical inference, to data-driven machine learning from examples and correlations
  - A unified paradigm: logic merges with statistics and neuro-science
- The Internet reaches maturity:
  - From an infrastructure for human communication to a global interconnected data infrastructure,
  - From access to passive information to active algorithmic intermediation

AI and the Internet: convergent successes

- AI: From toy examples to a host of real applications:
  - speech and image recognition, question-answering, recommendation, translation, planning, autonomous mobile robots, etc.
- The Internet: From message exchanges to the universal medium for any private and public services
  - shopping, banking, pay taxes, get benefits, information seeking, access to knowledge, social networking, etc.

What AI does and wants



- What AI does
  - apply learning methods to vast sets of examples to discover correlations
  - make classifications and predictions based on correlations and data
  - learn from past successes and failures in classifying and predicting

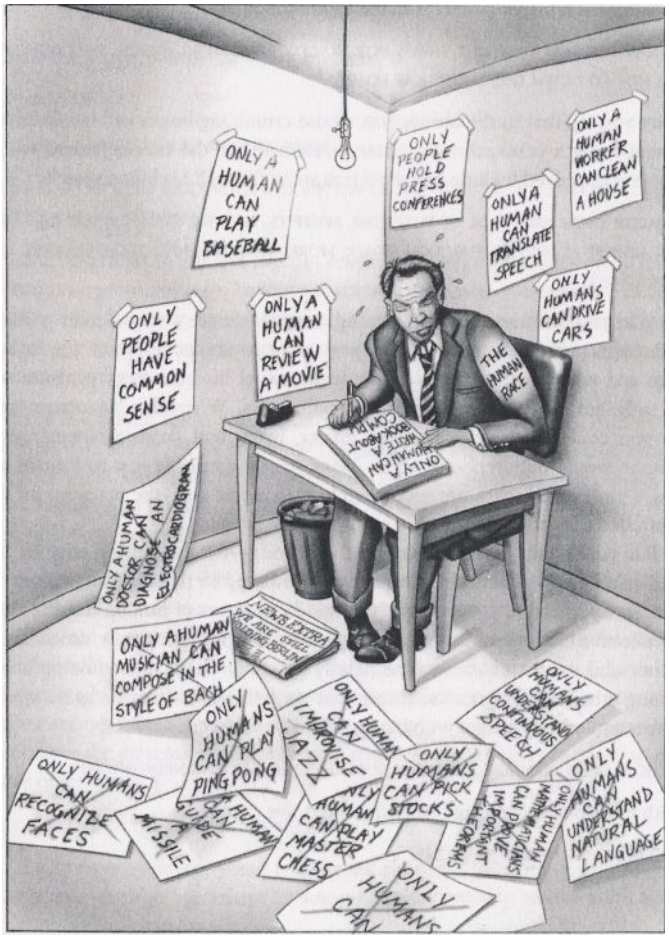
- What AI wants
  - the largest sets of examples
  - Including as much data as possible to discover new correlations

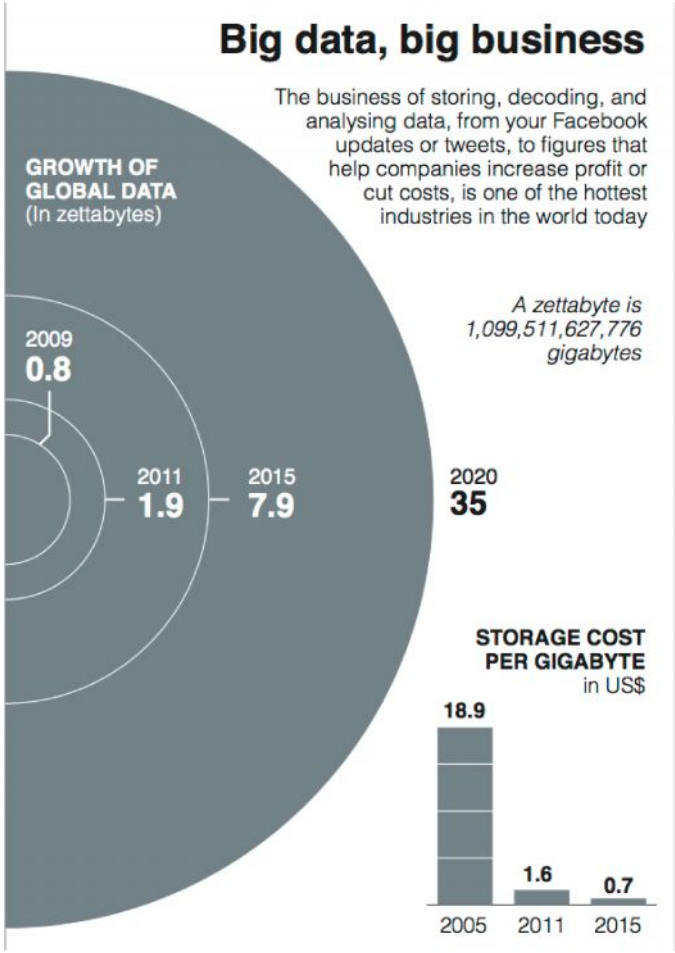
What the Internet does and want

- What the Internet does
  - enable human interaction
  - link billions of connected devices
  - collect all kind of data from physical and virtual environments
- What the Internet wants
  - services, providing intelligent and individualised solutions
  - the ability to extract useful knowledge from data

The great convergence

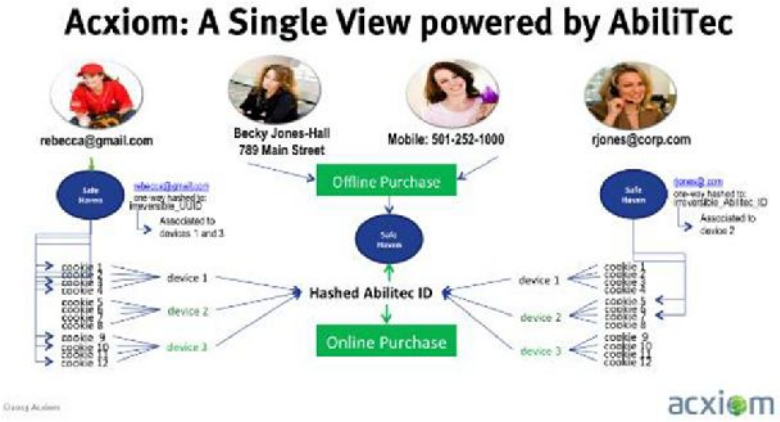
- The Internet provides AI with data
- AI enables the Internet to exploit the data





Data-hungry AI meets data-abundant Internet

- Pervasive data collection
- Learning from big data
- Ubiquitous algorithmic intelligence

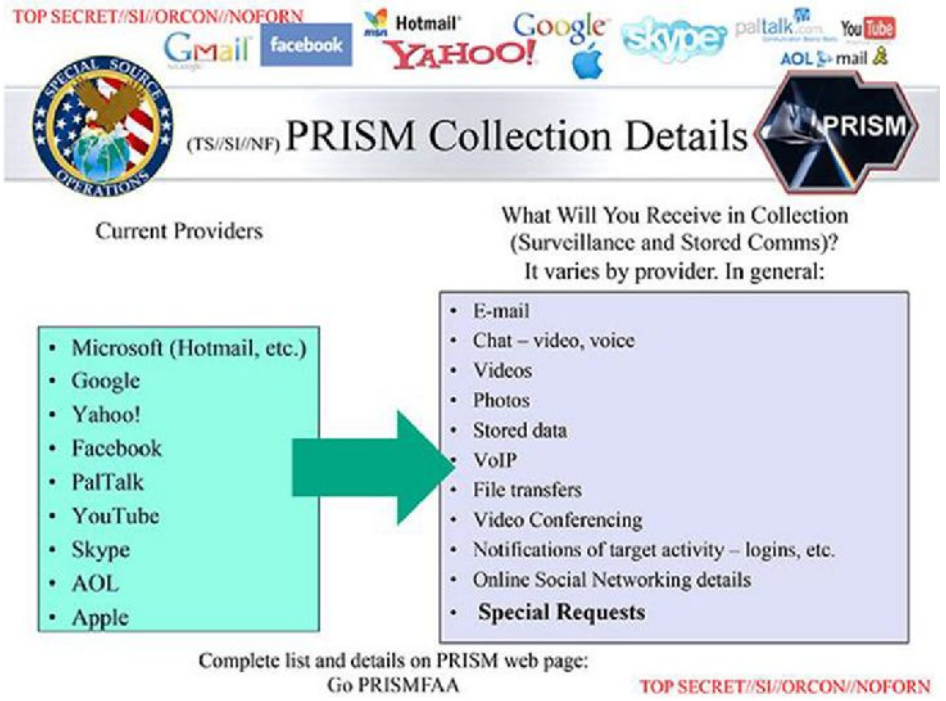


The Internet & AI: the promise

- overcome the information overload
- world-wide generation and distribution of knowledge and solutions
- economic efficiency, wealth creation
- cost-effective, individualised private and public services
- environmental-friendly management of utilities, traffic, logistics
- support for transparency, overcome bias and discrimination
- Etc.

The Internet + AI infrastructure: The catch

- Data collection/analysis/surveillance
- We cannot get out of the infrastructure
- We cannot effectively resist/contest influence and manipulation



Ethics and law violations by AI + Big Data

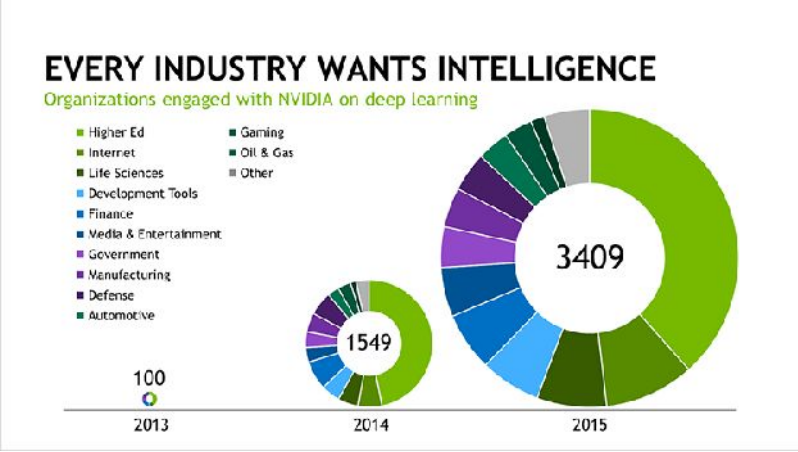
By 2018, 50% of violations of business ethics will be performed by algorithms

Gartner 2016

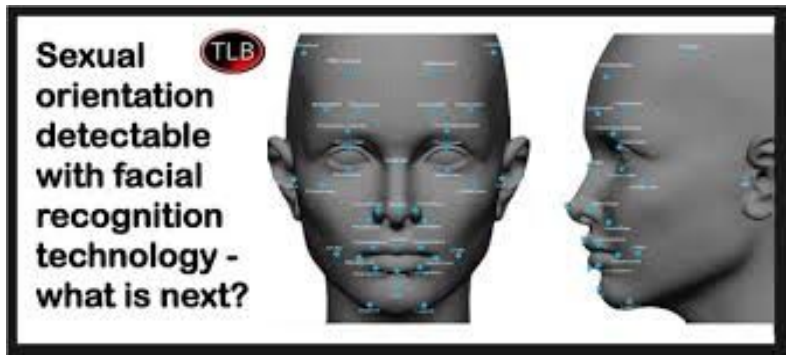
What drivers for AI

AI is in principle innocent, it only pursue the goals it is assigned

- By profit-making actors
  - Efficiency, cost reduction, better services
  - Anticipate/control/direct behaviour (to sell goods and services)
  - Two sided markets: capture user, to send them advertising, suggestions, and services, get revenue from advertisers-persuaders
- By governmental actors
  - Efficiency, costs reduction, better services
  - Anticipate/control/direct behaviour (for security and other purposes)



But impacts on individual and society are not always good!



Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

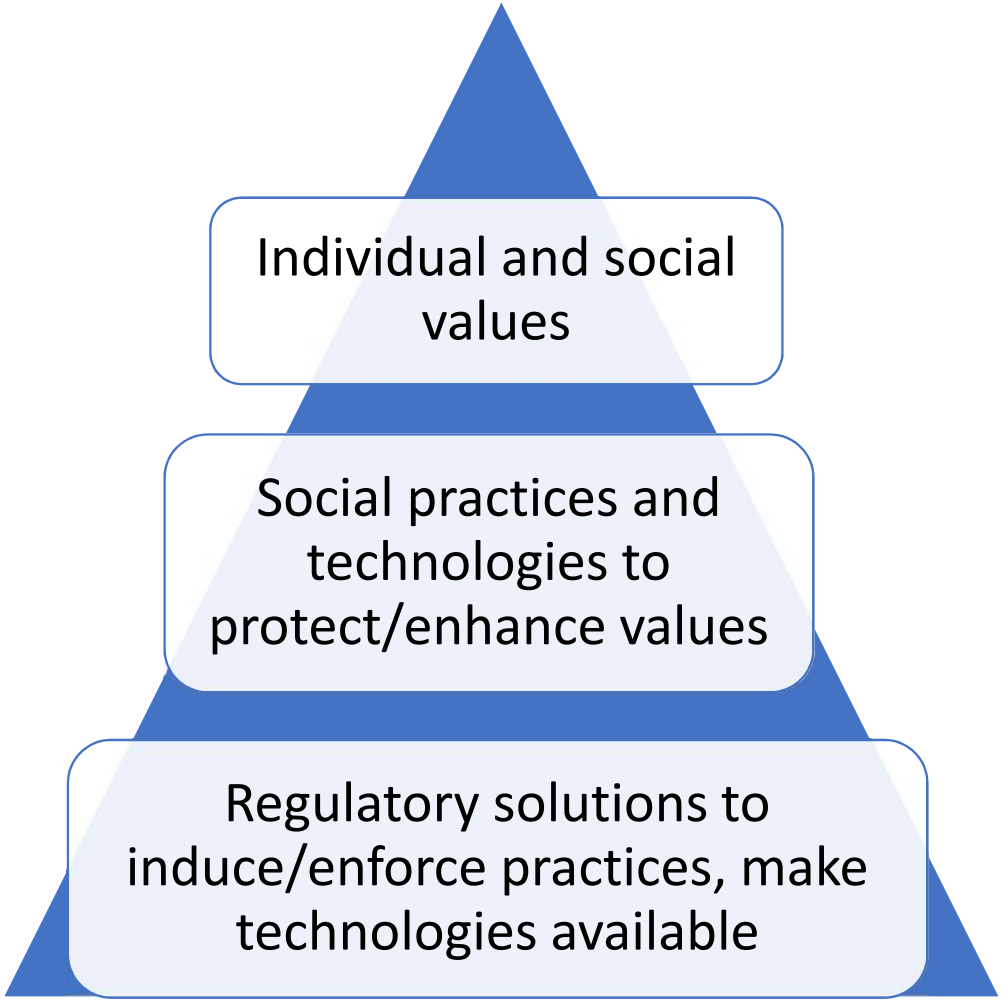
What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

A value-based approach to regulating AI



A disrupting flow of innovations, generates multiple and diverse legal/social issues

How to proceed:

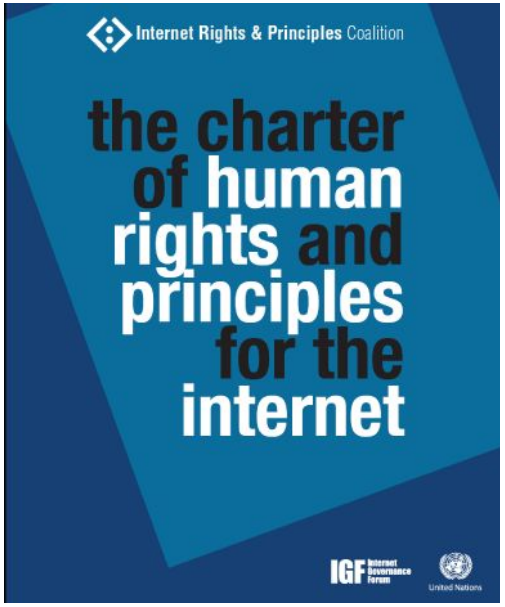
- Start from first principles
- Promote valuable socio-technical practices through tailored regulations and technologies
- Adapt existing legal frameworks, multi-layered regulation

What answers?

- Regulation
  - Smart regulation to direct the use of AI by private and public organisations
    - https://artsy.eui.eu/
- Empowerment
  - Make the power of AI available to citizen and civil society
    - https://claudette.eui.eu/

The legal-ethical framework: rights and social values

- Human/fundamental rights:
  - privacy, data protection, dignity, autonomy, freedom of expression, non-discrimination, equality, participation
- Social/economic goals:
  - welfare, competition, efficiency, science, art and culture, cooperation, civic dialogue, democracy



The legal framework: Multiple sectorial legal regimes and principles

- Data protection law
  - Principles: lawfulness, fairness and transparency; purpose limitation; data minimisation, accuracy; integrity and confidentiality; accountability; legitimate interest, data subject rights, etc.
- Consumer protection law
  - Principles: Protection of the weaker party, Regulated autonomy, Non-discrimination, etc.
- Competition law
  - Principles: fair competition, consumer welfare, etc.

Synergy and tensions: EDPS (Opinion 8/18)

- **Consumer** and **data protection law** share common goals of **redressing imbalances of informational and market power**
- Together with **competition law**, data protection and consumer protection need to work to ensure that people are **treated fairly**.

An issue: are personal data a tradable property?

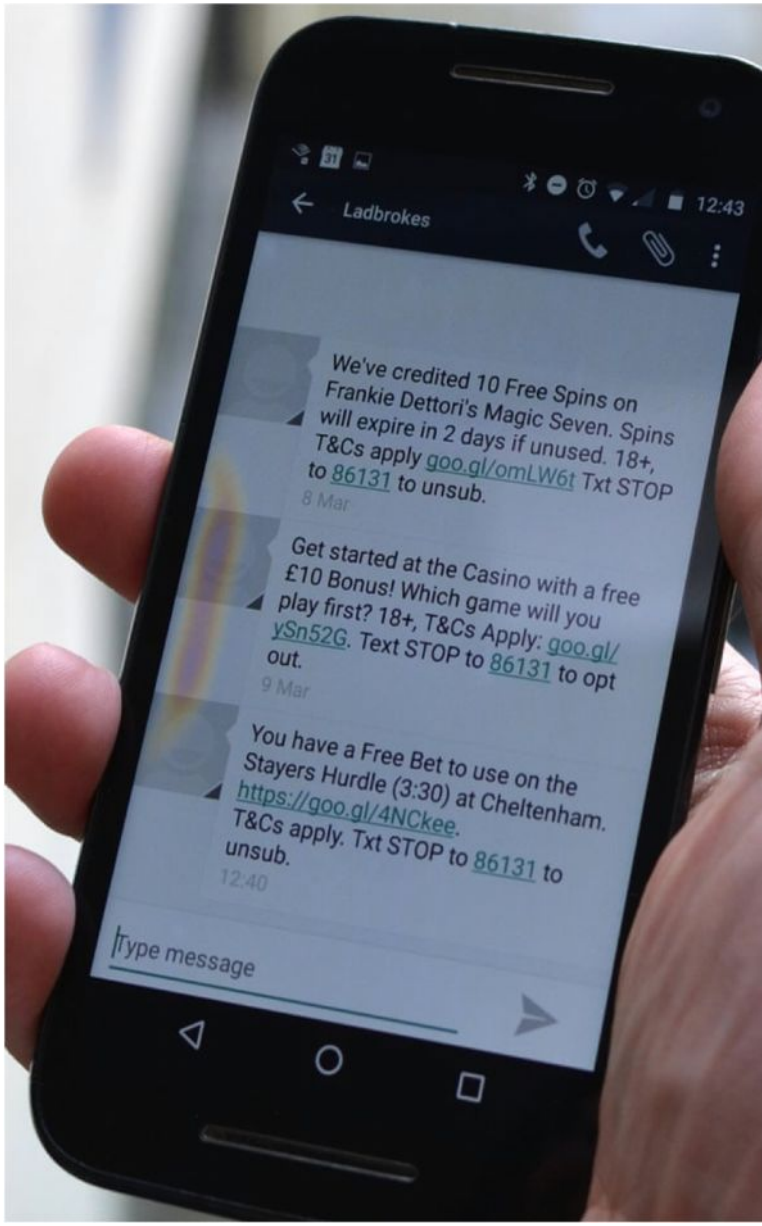
- Can a consumer pay with his or her data? What about revocable consent under GDPR? What about privacy as a fundamental right?

What interests/rights are at stake

- Privacy-data protection
  - to lawful and proportionate processing of personal data, to control processing
- Fair algorithmic treatment
  - not to be subject to unfair differentiated treatment
- Algorithmic transparency
  - to know why a certain algorithmic response or decision ha been given
- Interest in fair algorithmic interaction
  - not to be misled or manipulated
- Interest in fair algorithmic (cognitive) competition
  - Interest in accessing data sources and algorithms that are available to big players

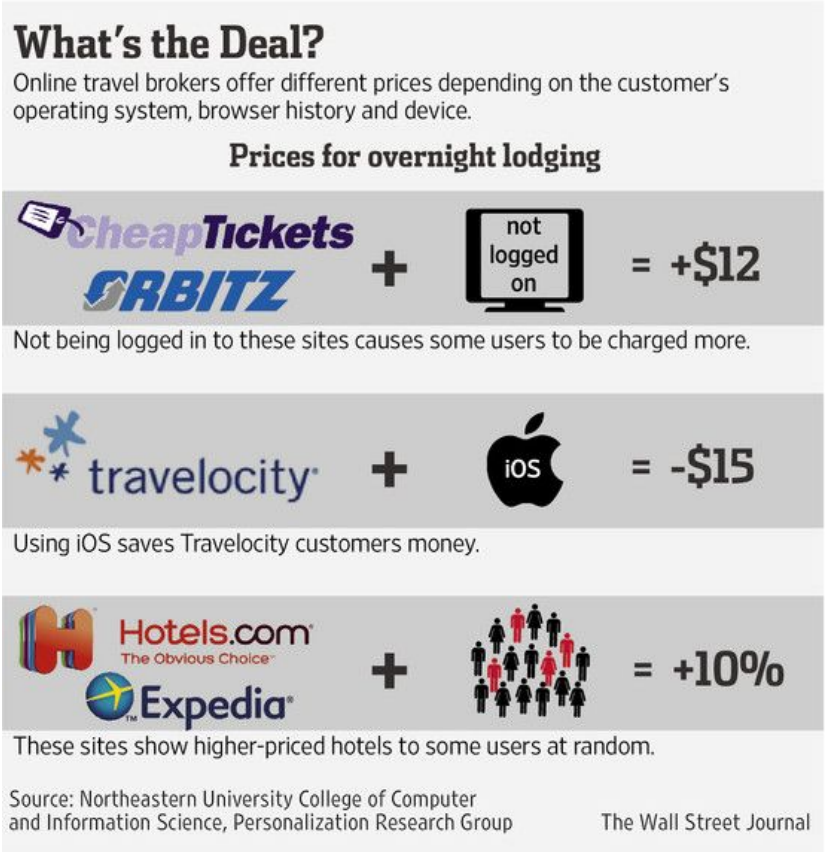
Focus on risks for consumers

- Unfair algorithmic decisions
- Unfair, excessive data processing/profiling
- Limitations on consumers' autonomy
- Discriminatory/unfair/ aggressive/exploitative advertising
- Filter bubbles/echo chambers
- Information asymmetry; arbitrary power
- Exploitation of vulnerabilities
- Opacity, inability to contest
- Risk of erroneous diagnoses, suggestions



Issue: Price discrimination

- AI enables sellers to figure out the highest price a client can pay
- Should there be price discrimination in consumer retail markets? For what good/service, on what grounds'?
  - cost structures, risks
  - spending capacity, needs, interests, vulnerabilities
- Normative standards:
  - Consumer protection law: is it unfair/discriminatory?
  - GDPR: is it an automated decision, is there a legitimate interest?
  - Competition law: does this affect competition?

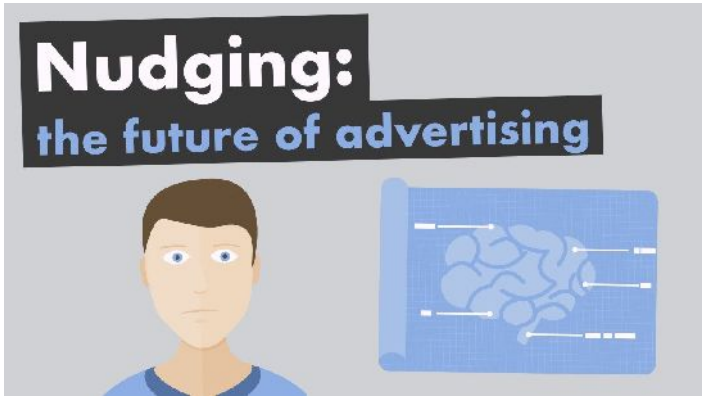


Issue: Discrimination in algorithmic offers

- What if different people are offered different opportunities
  - Men getting better loans, women better insurance
  - People of certain ethnicity being more often refused opportunities
- What if the AI system has “innocently” learned to apply differential treatment
  - based on previous practice
  - to achieve a business purpose
- What legal solution
  - Data protection law: legitimate purpose, sensitive data, consent?
  - Consumer protection law/discrimination law: unacceptable discrimination?

Issue. Targeted advertising/malicious nudging

- AI can deliver each consumer the ads that most trigger purchasing, depending on:
    - how well they match consumer's needs and interest
    - how well they exploit consumer's vulnerabilities (e.g., predatory loans to people in difficulties, gambling offers to gambling addicts, drugs to depressed people)
- What legal solution?
    - When is it permissible? When a prevailing "legitimate interest"?
    - When does it "materially distort the economic behaviour of consumers"



Issue: Aggressive personalised advertising

- What if personalized advertising, to maximize clicks and revenues, exploit individual vulnerabilities (economic hardship, propensity to gambling, etc.)
  - This may be non-intentional, as the system may aim to use any factors correlated to clicks and purchases, regardless of the impact on consumer's interests
- Data protection law: Is exploiting vulnerabilities acceptable?
- Consumer protection law: does it count as "aggressive advertising"

Issue: Discrimination in Ad delivery

- Systems meant to address Ads and offers to those who are most probably interested in them may reproduce biases and discrimination
  - Offers for top jobs to male people
  - Offers for houses to those who match current ethnic ownership

- Maybe no data protection issue
- But is there a discrimination issue?


theguardian

ort football opinion culture business lifestyle fashion environment tech

Women less likely to be shown ads for high-paid jobs on Google, study shows

Automated testing and analysis of company's advertising system reveals male job seekers are shown far more adverts for high-paying executive jobs

Issue: “Turn off” personalization?

- Personalised treatment of consumer can provide the with advantages, but also disadvantages
- Should the consumers know that they profiled, for what specific purposes?
- Should consumers be offered the option to trade and purchase anonymously?

- The GDPR allows consumer to withdraw consent and object to profiling. Is there a right to trade anonymously?

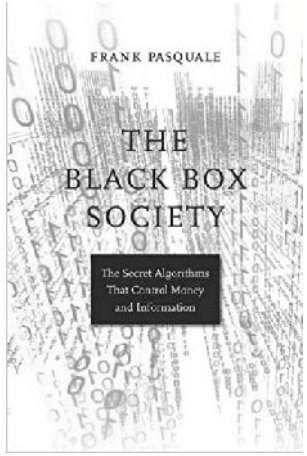
Issue. Rights to information/transparency

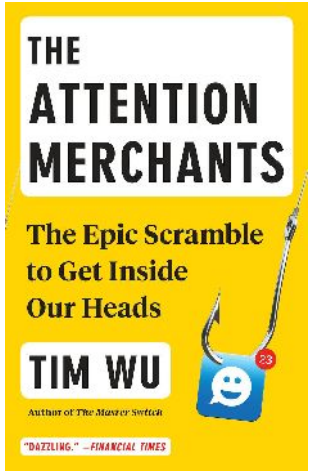
- Have (should have) consumers a right to know that they are offered personalised prices? Calculated in what way?
- Have (should have) consumers a right to know to know that their treatment is dependant on the tracking of their behaviour, and on consequent classifications/profiling? With what impacts?

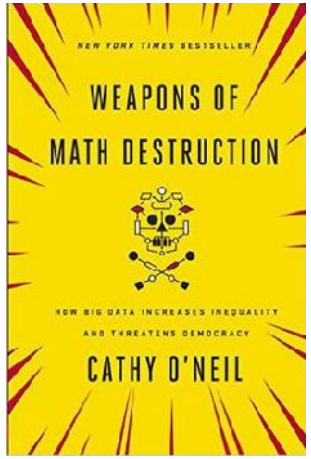
- Data protection law: information obligations on data controllers
- Consumer protection law: information obligations on suppliers
- What about platforms?

Other issues to be addressed

- Right to procedural regularity
- Right to substantive legality
- Right to explanation/justification
- Right to have a human answer
- Right to be protected from abusive manipulation
- Liabilities for mistaken decisions/advice







Empowering civil society?

- Remedy the imbalance for AI-powered platforms and suppliers through citizen and consumer-empowering AI
  - Protection against unwanted monitoring
  - Support in detecting unfair/unlawful use of AI
  - Control over fairness of commercial practices
- Some examples:
  - Spam filters
  - Ad-blocking tools
  - Anti-tracking tools
  - Price comparison platforms
  - Detection of, and response to, violations of law and ethics
- Should consumer-empowering initiatives be supported and incentivised?

Detect, and respond to, violations of law and ethics

- AI can contribute to address online violations:
  - Unlawful and unethical behaviour on line is often unnoticed, rarely acted upon.
  - AI can facilitate cost-effective prevention/detection/reaction
- The AI-empowerment should be available to those who most need it:
  - Commercial actors, and resourceful individuals already use AI to apply the law
  - This opportunity should be open to citizens and civil society!

What about privacy policies and terms of service?

- Most online terms of service and privacy policies contain unlawful/unfair clauses, or miss relevant information:
  - Consumers agree but don't read
  - NGOs (consumer organisations) lack resources

- AI can contribute:
  - AI support to citizens and civil society to detect and react
  - An example: An automatic detector of unfair clauses in online contracts and privacy policies: https://claudette.eui.eu/

CLAUDETTE GDPR

— Automatically Monitoring Privacy Policies —

Thanks for your attention

Giovanni Sartor, European University Institute / University of Bologna